

DETERMINING BETWEEN REQUESTS FROM THE WAN AND THE LAN

Claim 1 calls for a controller that determines whether a request to perform predetermined processing came in from the WAN or the LAN; and claim 11 calls for the step of determining whether a request to perform predetermined processing came in from the WAN or the LAN.

Susaki fails to disclose this feature because Susaki fails to discuss the WAN, and Shitama treats requests that come in from the WAN and the LAN the same.

Susaki discloses a client server system where a terminal 1 and a server 2 are connected through a communication network 3 such as a LAN (Fig. 1 and col. 5, lines 8-12). Susaki fails to provide any mention with regard to the WAN, and col. 9, lines 38-48 cited on page 2 of the Office Action fails to mention the WAN.

Shitama merely disclose a device that receives data from a WAN and transmits the data to the LAN. Therefore, even if Susaki and Shitama were combined as suggested in the Office Action (which Applicants do not admit would have been obvious), data from the WAN would be transmitted to the LAN, and would be processed the same as if the data came in from the LAN. Therefore, the combination of Susaki and Shitama would not need to determine whether requests come in from the WAN or the LAN, or need to determine whether a request to perform predetermined processing came in from the WAN or the LAN as called for by claims 1 and 11, for the additional processing called for by claims 1, 11 and 20.

REQUESTS FROM THE LAN

Claim 1 calls for a controller that automatically accepts an operation according to the request every time that it is determined that the request came in from the LAN; claim 11 calls for the step of automatically accepting an operation according to the request every time that it is determined that the request came in from the LAN; and claims 20 calls for a controller that

automatically performs predetermined processing according to a request every time that a performance of an operation is requested by a LAN.

Susaki fails to disclose this feature because a user authenticates some of the requests that come in from the LAN, and Shitama fails to discuss how requests are processed if they come in from the LAN.

Susaki discloses a client server system where a terminal 1 and a server 2 are connected through a communication network 3 such as a LAN (Fig. 1 and col. 5, lines 8-12). Susaki is directed to controlling access to a particular service by a user connected via the LAN in order to avoid leakage of official secrets and falsification of information (col. 1, lines 31-37). In order to achieve this, Susaki at col. 9, line 38 - col. 10, line 16 discusses using a service approval request processor 206 that determines if approval is required based on a process control rule. Based on the process control rule, a determination is made whether approval is not required (col. 9, lines 58-67), or if approval is required (col. 10, lines 1-16). Because approval may be required, Susaki fails to automatically accept requests that come in from the LAN as called for by independent claims 1, 11 and 20.

Shitama fails to discuss how requests are processed if they come in from the LAN because Shitama is instead directed to authenticating requests that come in from the WAN. Page 5 of the Office Action states "all requests from the LAN are trusted" and "implicitly allows all local requests for local resources". Although Shitama does disclose a LAN, Shitama fails to explicitly provide such disclosure.

Furthermore, pages 12 and 13 of the Office Action asserts that "it does not hold that all of the levels of scrutiny must be used in a combination with Shitama" and that "requests from the LAN are always fulfilled"; therefore, in combination with Susaki, one skilled in the art would "place all LAN address as having a user authority level of "0" in the table of Fig. 5." Applicants disagree. It is not reasonably predictable to discard the security provided for

requests that come in from the LAN as discussed by Susaki and to only apply it to requests that come in from the WAN in the manner suggest on pages 12 and 13 of the Office Action.

Applicants assert that, given the detail provided by Susaki as to how requests from the LAN are processed and the lack of detail provided by Shitama, one skilled in the art combining the disclosures of Susaki and Shitama would logically treat requests from the LAN as disclosed by Susaki (that is, some requests that come in from the LAN would require user approval). In other words, one skilled in the art would not automatically accept an operation according to the request every time that it is determined that the request came in from the LAN as called for by claim 1, for example. Furthermore, if one skilled in the art were to combine Susaki and Shitama (which Applicants do not admit would have been obvious), one skilled in the art would instead add the security for requests that come in from the LAN as disclosed by Susaki to the security for requests that come in from the WAN as disclosed by Shitame. Such a combination fails to suggest all of the features of independent claims 1, 11 and 20.

REQUESTS FROM THE WAN

Claims 1 and 20 call for a controller that allows a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN; and claim 11 calls for the step of allowing a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN.

As discussed above, Susaki only discloses a client server system where the terminal 1 and server 2 are connected through a communication network 3 such as a LAN (Fig. 1 and col. 5, lines 8-12). Susaki never discusses the WAN, and the citations provided in the Office Action, for example on page 2, fail to discuss the WAN.

Shitama limits access from the WAN to the LAN by using a gateway 30 that authenticates all requests from the WAN using a predetermined authentication code and method. Shitama fails to provide any discussion with regard to allowing any user intervention. Therefore, Shitama suffers the same problems identified in paragraph [0003] of Applicants' specification in that passwords may be artificially leaked to outsiders as well as being leaked by stealing packets from a network.

For similar reasons discussed above, Applicants assert that, given the detail provided by Shitama as to how requests from the WAN are processed and the lack of any detail by Susaki, if one skilled in the art were to combine Susaki with Shitama, which Applicants do not admit would have been obvious, then one skilled in the art would have used Shitama's authentication procedure for requests that come in from the WAN. It would not have been reasonably predictable to discard Shitama's procedure for requests from the WAN in order to use Susaki, which is directed to requests from the LAN. Again, if one skilled in the art were to combine Susaki and Shitame (which Applicants do not admit would have been obvious), one skilled in the art would instead add the security for requests that come in from the LAN as disclosed by Susaki to the security for requests that come in from the WAN as disclosed by Shitame.

In addition, even if one skilled in the art would have used Susaki's procedure with Shitama, the combination still fails to suggest allowing a user of the communication device to determine whether the operation according to the request is accepted or rejected every time that it is determined that the request came in from the WAN as called for by claim 1, for example. As discussed above, Susaki allows a user to authenticate some requests and Shitama uses the gateway to authenticate all requests.

* * * * *

In view of at least the above, the combination of Susaki and Shitama fails to disclose or suggest all of the features in the independent claims as well as the features in the dependent claims. It is respectfully requested that the rejection be withdrawn.

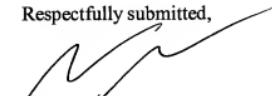
Claims 2 and 12 were rejected under 35 U.S.C. §103(a) over Susaki in view of Shitama and Joubert et al. (Joubert), U.S. Patent No. 6,101,616, claims 5 and 14 were rejected under 35 U.S.C. §103(a) over Susaki in view of Shitama and Allen et al. (Allen), U.S. Publication No. 2003/0041333, and claims 10 and 19 were rejected under 35 U.S.C. §103(a) over Susaki in view of Shitama and Boehmke et al. (Boehmke), U.S. Publication No. 2002/0126822. The rejections are respectfully traversed.

None of Joubert, Allen and Boehmke overcome the deficiencies of Susaki and Shitama as applied to independent claims 1, 11 and 20. It is respectfully requested that the rejections be withdrawn.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,



James A. Oliff
Registration No. 27,075

Scott M. Schulte
Registration No. 44,325

JAO:SMS

Date: December 2, 2008

OLIFF & BERRIDGE, PLC
P.O. Box 320850
Alexandria, Virginia 22320-4850
Telephone: (703) 836-6400

<p>DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Charge any fee due to our Deposit Account No. 15-0461</p>
--